Секция «Глобальная безопасность»

Прогнозирование и построение маршрутов НСД злоумышленников в зонной модели физической защиты информационных объектов на базе нейросетей

Научный руководитель – Соляной Владимир Николаевич

Цвырко Снежана Олеговна
Студент (бакалавр)
Технологический университет, Королёв, Россия
E-mail: tsnwork@mail.ru

В работе решается одна из **ключевых задач** успешного функционирования критического объекта - быстрая, эффективная защиты от возникающих угроз, среди которых следует особо выделить **незаконные действия физических лиц:** на заданную охраняемую территорию защищаемого критического объекта происходит незаконное проникновение; требуется рассчитать и продемонстрировать область, в которой предполагаемо находится злоумышленник в конкретно заданный момент времени в интересах обоснования оптимальных путей передвижения оперативных групп реагирования.

Последствия их воздействия непредсказуемы и широко варьируются: от хищения имущества предприятия до создания чрезвычайных ситуаций на защищаемом критическом объекте. В этих условиях безопасность предприятия должна отвечать принципам **«разумной достаточности»**, **«эффективность - стоимость»**, а также теоретически разработанной и практически применяемой концепции физической безопасности предприятия.

Решаются ключевые **цели**: повышение эффективности перехвата злоумышленника, снижение ожидаемого ущерба (рисков) от нарушителей за счет моделирования оптимальных действий служб безопасности и разработка прикладного программного комплекса.

Научная новизна проекта заключается в применении методов хромоматематики, использовании зонно-рубежного отображения перемещения злоумышленника и рекурсивных алгоритмов оптимизации. Также имеются большие **перспективы коммерциализации** (**практическая значимость**): возможно создание ППО с целью улучшения эффективности систем физической защиты критически важных объектов, поскольку существующие программные средства по ряду параметров уступают предложенной разработке; планируется выход на рынок систем охраны.

Под нарушителем будем понимать лицо или группу лиц, которые в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности. Приказом министерства промышленности и энергетики РФ от 04.05.2007 №150 «Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики» определены шесть различных типов нарушителей, используемые в базе данных проекта [1].

Перед началом работы был проведён комплексный анализ рынка. Выявлены следующие аналоги проекта: EASI, ASSESS, Спрут, Спрут-ИМ, «Вега-2», «Контрфорс».

Был выявлен ряд недостатков:

- Заложена жесткая тактика действий сил реагирования.
- Отсутствует база данных по реальным-тактико-техническим характеристикам ТСФЗ и ФБ, относящихся к чувствительной информации.
- Погрешности в расчетах.
- Произведено за рубежом.
- Государственные (не продаются).

Программный комплекс создан для работы в трех режимах моделирования:

1. Реальное.
2. Прогнозируемое.
3. Статестическое.

В первом случае на работу программы будут влиять различные факторы: действия сил экстренного реагирования, работа датчиков охранной системы объекта, выбранная модель злоумышленника и др. Во втором случае все эти факторы задаются искусственно, тем самым производится проверка территории защищаемого объекта на наличие уязвимостей и соответствие принципам физической безопасности. В третий режим ПАК переходит в случае "простоя", когда необходим набор статетстических данных.

Для анализа эффективности СФЗ используется метод качественной оценки эффективности EASI (Estimate of Adversary Sequence Interruption), количественно показывающий эффект от изменения параметров физической защиты. EASI - модель на уровне «пути», для защиты более крупных и сложных систем требуются усовершенствованные компьютерные модели [3].

Результатом проведенной научно-исследовательской работы стало создание пилотного варианта прикладного программного обеспечения на базе инновационного использования методов хромоматематики [2], рекурсивных алгоритмов на плоскости и "многослойности" представлений параметров для моделирования действий злоумышленника с целью улучшения эффективности систем физической защиты критически важных объектов любого профиля в условиях специфических особенностей их функционирования. Создан авторский алгоритм моделирования области предполагаемого нахождения и прогнозирования перемещения злоумышленника на защищаемой территории. Разработан прототип программного комплекса, позволяющий на первом этапе прогнозировать во времени действия злоумышленника с графическим отображением. Ведется разработка усовершенствованного алгоритма с учетом новых факторов: действий служб безопасности, учетом одновременных перемещений нескольких групп злоумышленников, расширением учитываемых факторов обстановки.

Источники и литература

1) Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ. — М.: Гостехкомиссия России, 1992.
2) Цвырко О.Л., Цвырко С.О. Основы хромоматематики. Монография. – Ишим: Изд-во ИГПИ им. П.П. Ершова, 2013. – 122 с.
3) Гарсиа, М: Проектирование и оценка систем физической защиты. Пер. с англ./М.Гарсиа-М.:Мир: ООО «Издательство АСТ», 2002.-386с.